Noviembre 19, 2009

Conferencias de OWASP AppSec:

Nov 17th-20th App Sec India

http://www.owasp.org/index.php/Category:India

Dec 2nd 2009 BeNeLux Day College De Valck
http://www.owasp.org/index.php/BeNe-Lux_OWASP_Day_2009

Dec 10th-11th IBWAS, Madrid

http://www.ibwas.com/

AppSec Research 2010 - Stockholm, Sweden

Miembros de Tabla de OWASP

Jeff Williams

Dinis Cruz

Dave Wichers

Tom Brennan

Sebastien Deleersnyder

Felicitaciones a los dos nuevos Miembros de la Tabla de OWASP:

Eoin Keary &

Matt Tesauro

OWASP
The Open Web Application Security Project

OWASP TOP 10 2010 RC1 - Dave Wichers

El OWASP Top 10 2010 RCI fue liberado en el evento AppSec DC. Wichers Dave, como líder del proyecto realizó la presentación. Ha subido tanto la presentación como el Top 10 en sí al wiki de OWASP. La presentación se encuentra en formato .pptx y el Top 10 en formato PDF.

Ambos pueden encontrarse en la parte superior de la página del proyecto del Top 10: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Dado que se trata de una versión candidata a liberación, se encuentra abierto a comentarios hasta el final del año. Así que, por favor revíselo y traslade sus comentarios a Dave Wichers.

Y el TOP 10 para el 2010 (RC1) es...

A1: Inyección
A2: Cross Site Scripting (XSS)
A3: Autenticación rota y la Gestión de la Sesión
A4: Referencia Insegura Directa a Objetos
A5: Cross Site Request Forgery (CSRF)
A6: Mala configuración de la Seguridad
A7: Fallo en la restricción de acceso a URL
A8: Redirecciones y Reenvios sin Validación
A9: Almacenamiento Cryptográfico Inseguro
A10: Capa insuficiente de Transporte

Esta actualización se basa en más fuentes de información de vulnerabilidades de Aplicaciones Web que en las versiones anteriores en donde se determinó el nuevo Top 10. También se presenta esta información de una forma más concisa, de manera convincente y mas digerible e incluye fuertes referencias a los muchos nuevos recursos disponibles que pueden ayudar a abordar cada cuestión, particularmente los nuevos proyectos OWASP Enterprise Security API (ESAPI) y Application Security Verification Standard (ASVS). Un cambio significativo para esta actualización será que el OWASP TOP 10 estará enfocado en el TOP 10 de las riesgos de Aplicaciones Web, no solo en las vulnerabilidades más comunes. http://www.owasp.org/index.php/OWASP_Top_10_2010_AppSecDC

OWASP AppSec USA 2009 Lorna Alamri

En la AppSec DC destacó Joe Jarzombek, Director de Software Assurance del Departamento de Seguridad Nacional - División de CiberSeguridad quien con su charla inaugural dio comienzo a la conferencia. Un panel de discusión compuesto de CISOs federales (Earl Crane-Jefa de División de Estrategia de Seguridad, DHS, Gary Galloway-Director Adjunto de la Oficina de Seguridad de la Información, Departamento del Estado, Timothy Ruland-CISO, Oficina del Censo de EE.UU., y Richard Smithon-CISO TSA cubrieron temas tales como:

- Nivel de Madurez del Programa de Seguridad de Aplicaciones
- Integración de la seguridad de aplicaciones dentro de Frameworks de Seguridad Existentes
- Creando un Grupo de Seguridad de aplicaciones
- Web 2.0
- Transparencia

Otro panel muy concurrido estuvo en el asegurar el proceso SDLC y la importancia de refuerzo de la seguridad en el software, los miembros del jurado fueron: Dan Cornell, Michael Craigue, Dennis Hurst, Joey Peloquin y Keth Turpin. Pravir Chandra asistió como asesor.

OWASP AppSec DC fué el evento de la App Sec en EEUU para el 2009.

OWASP Podcasts Series

Presentado por Jim Manico

Sandro Gauci (wafwoof)

Michael Coates (Real Time Defensese, OWASP AppSensor)

Eladad Chai (Ataques de Negocio Lógicos)

Andrés Riancho (OWASP w3af)

Giorgio Fedon

OWASP Development Guide—Andrew van der Stock

Mike Boberski es el nuevo Project Manager de Desarrollo y Guía. Otras aportaciones de Mike en OWASP incluyen el "*Application Security Verification Standard*", varios "*cheatsheets*", y ESAPI para PHP.

Sus funciones incluirán:

* Coordinación de voluntarios - asignación de trabajos, etc.

* Mantener el Proyecto de la Guía Wiki, páginas, road maps, etc

* Control de Calidad.

Andrew van der Stock propone que la Guía de Desarrollo pase a ser la guía detallada de diseño para los requerimientos de los estándares de seguridad de aplicaciones. Como mínimo, le gustaría cubrir cada control único mencionado en el ASVS.

El Plan:

1. Ruta de trabajo con realismo en la línea de tiempo
2. Llamado a voluntarios

http://www.owasp.org/index.php/Category:OWASP_Guide_Project

Mike.boberski@owasp.org

NIST SP 800-David Campbell

Rex Booth de la Comisión de Industria organizó con éxito una propuesta a principios de este año para presentar comentarios coherentes para la 3 ª revisión de la publicación especial de NIST 800-53 publicado recientemente. Los federales reconocerán este documento, titulado "*Controles de seguridad recomendados para los Sistemas de Información Federal y Organizaciones*" como el corazón y el alma de FISMA, que es el proceso por el cual las agencias federales se ganan los "grados de letra" de infosec.

Nos sentimos muy complacidos de ver que varias de las revisiones y actualizaciones proporcionadas por OWASP se incluyeron en el documento liberado.

El Comité Global de la Industria continua dando seguimiento a los proyectos de documentos liberados por el NIST y otras organizaciones pertinentes y proporciona información para asegurar que la comunidad AppSec está propiamente representada.

AppSec DC 2009 Sala de exposiciones y el servicio de pasillo.

Enterprise Security API - Noticias del proyecto

Noticias del proyecto

- El desarrollo de la versión Python de ESAPI dará comienzo pronto. Por favor, contactar con jeff.williams@owasp.org para más información.
- ESAPI Java 2.0 está apunto de completarse. Se lanzará en las próximas semanas. Por favor, comprobar el SVN y enviar cualquier petición de última hora a la lista de ESAPI.
- Se ha pedido una edición Coldfusion de ESAPI. Si hay algún desarrollador interesado, por favor contactar con jeff.williams@owasp.org y ofrecerse como voluntario.
- ESAPI ha sido sometido a una revisión línea por línea por un importante integrador de sistemas. Se publicará todo lo que se ha encontrado pronto pero no son de mayor importancia.
- OWASP ESAPI ha sido integrado dentro del OWASP Secure Software Contract Annex en el proyecto OWASP Legal Project.
- OWASP ESAPI será presentado por Jeff Williams en el evento OWASP Software Assurance Day DC 2009 junto con el Software Assurance Forum patrocinado por el Departamento de Seguridad Nacional de los Estados Unidos, el Departamento de Defensa y el Instituto Nacional de Tecnología y Estándares.

Lista de correo del proyecto

Subscríbete aquí
Comienza a utilizarla aquí

Estado semanal

- ESAPI Doc Weekly Status 2009-11-13.pdf

Para las noticias más actuales del proyecto:

http://www.owasp.org/index.php/

Nubosidad con posibilidad de 0 -Day.
Comienzo de la presentación dada por Jon Rose y Tom Leavey de Trustwave/Spiderlabs.

Hazte miembro

La asociación profesional de la Fundación OWASP es una organización (501c3) sin ánimo de lucro no asociada con ningún producto o servicio comercial. OWASP es un proyecto libre dedicado a la búsqueda y lucha contra las causas del software inseguro, y para resultar satisfactoria necesitamos su apoyo. Los miembros de OWASP, con el apoyo educacional y comercial de la organización, forman una comunidad de seguridad en aplicaciones que trabajan conjuntamente para crear artículos, metodologías, documentación, herramientas y tecnologías ("Materiales OWASP") - Powerpoint de Membresía 2009

¿Por qué convertirse en miembro?

- Como miembro de la comunidad de internet, ¿está de acuerdo con la ética y los principios de la Fundación OWASP?
- ¿Quiere resaltar su conocimiento sobre seguridad en las aplicaciones web?
- ¿Quiere seguir aumentando su conocimiento y ampliar sus habilidades consiguiendo descuentos en conferencias OWASP?
- ¿Quiere expandir su red personal de contactos? Grupo Linked'In de OWASP

Una parte de su cuota como miembro se destinará al apoyo de un capítulo local de su elección.

Contacto: Kate Hartmann

Kate.Hartmann@owasp.org

"Como resultado directo de la conferencia AppSec DC 2009, OWASP consiguió 70 nuevos miembros."
Kate Hartman

Fundación OWASP
9175 Guilford Road
Suite #300
Columbia, MD 21046

Teléfono: 301-275-9403
Fax: 301-604-8033
E-mail:
Kate.Hartman@owasp.org

La comunidad libre y abierta de seguridad

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas la herramientas, documentos, foros y capítulos de OWASP son gratuitos y abierto a cualquiera interesado en mejorar la seguridad de aplicaciones. Abogamos por resolver la seguridad de aplicaciones como un problema de gente, procesos y tecnología porque las soluciones mas efectivas incluyen mejoras en todas estas áreas. Nos puede encontrar en www.owasp.org.

OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva.

OWASP no está afiliada a ninguna compañia de tecnología, aunque soportamos el uso informado de tecnologías de seguridad comerciales. Parecido a muchos proyectos de software de código abierto, OWASP produce muchos materiales en una manera abierta y colaborativa.

La Fundación OWASP es una entidad sin ánimo de lucro para asegurar el éxito a largo plazo del proyecto .

Noticias del Proyecto OWASP
Paulo Coimbra, Manager del Proyecto OWASP

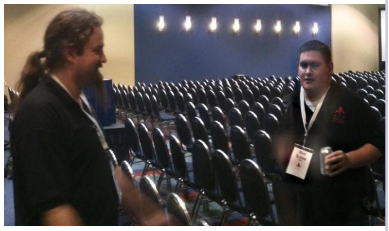
Proyectos nuevos;

OWASP Security Assurance Testing of Virtual Worlds, dirigido por ***Rick Zhong***.

Actualizaciones:

El proyecto OWASP Content Validation using Java Annotations Project ha lanzado su primera version (SHIP Validator 0.3 Release) la cual está lista para ser evaluada y su liderazgo está buscando activamente a un líder del Proyecto o del Capítulo para actuar como Primer Revisor.

El proyecto **The OWASP EnDe Project** http://www.owasp.org/index.php/Category:OWASP_EnDe#tab=Project_Details acaba de lanzar una nueva version, que corresponde con la 0.1.68.



Doug Wilson y Mark Bristow preparándose para el comienzo del AppSec DC 2009. Rex Booth detrás de la cámara.

Newsletter Editor: Lorna Alamri
Special thanks to Rex Booth for photos, Adam Baso for editing help and Colin Watson for content suggestions.